COMBINED INTEROPERABILITY TECHNICAL ARCHITECTURE (CITA)

ACP140 (A)

JULY 2001

FOREWORD

1. The Combined Communications-Electronics Board (CCEB) is comprised of the five member nations, Australia, Canada, New Zealand, United Kingdom and United States and is the Sponsoring Authority for all Allied Communications Publications (ACPs). ACPs are raised and issued under common agreement between the member nations.

2. ACP140 (A), COMBINED INTEROPERABILTY TECHNICAL ARCHITECTURE (CITA), is an UNCLASSIFIED CCEB publication.

3. This publication contains Allied military information for official purposes only.

4. It is permitted to copy or make extracts from this publication.

5. This ACP is to be maintained and amended in accordance with the provisions of the current version of ACP198.

THE COMBINED COMMUNICATION-ELECTRONICS BOARD
LETTER OF PROMULGATION
FOR ACP 140(A)

1. The purpose of this Combined Communication Electronics Board (CCEB) Letter of Promulgation is to implement ACP 140(A) within the Armed Forces of the CCEB Nations. ACP140 (A), COMBINED INTEROPERABILITY TECHNICAL ARCHITECTURE (CITA), is an UNCLASSIFIED publication developed for Allied use and, under the direction of the CCEB Principals. It is promulgated for guidance, information, and use by the Armed Forces and other users of military communications facilities.

2. ACP140 (A) is effective on receipt for CCEB Nations and when directed by the NATO Military Committee (NAMILCOM) for NATO Nations and Strategic Commands. When effective, ACP140 is to be destroyed in accordance with national security regulations.

EFFECTIVE STATUS

Publication	Effective for	Date	Authority
ACP140 (A)	CCEB	5 Nov 2001	LOP

3. All proposed amendments to the publication are to be forwarded to the national co-ordinating authorities of the CCEB or NAMILCOM.

For the CCEB Principals:

N. CRAM
Squadron Leader
Permanent Secretary
CCEB

RECORD OF MESSAGE CORRECTIONS

Identification of Message Correction and date time group.		Date Entered	By whom entered
DTG	Message Correction		
	1/1	1 March 2002	CCEB-PS

TABLE OF CONTENTS

This page intentionally blank

CHAPTER 1

GENERAL

SECTION I - INTRODUCTION

101. BACKGROUND

Fundamental to the definition of interoperability is an understanding of the operational environment within which the CCEB nations will operate and in which interoperability must be achieved.

The operational environment of the future is perceived to be one of coalitions, flexible in their constitution and unlikely to be constrained to CCEB members. Partners will not have common procedures and operational techniques. The operational environment will also need to take into account civil and national influences and the integration of functional elements at all levels of the organisational structure.

The essence of combined interoperability is the ability to integrate command and control systems within this coalition structure. This requirement is the ability to share and actively exploit common information while dynamically developing processes and procedures that are appropriate to the existing coalition.

102. CCEB VISION

The CCEB vision statement adopted by the Principals which describes the goal environment is:

> *"The CCEB is committed to maximising the effectiveness of combined operations by the definition of a Combined Interoperability Environment. This environment will enable users to share, creatively apply and add value to collective information and knowledge, constrained solely by policies defined by originators and recipients."*
>
> *(*CCEB Publication 1 Ver 3.1 dated 11th Aug 2000*)*

The Combined Interoperability Environment goal is to establish an interoperable Communications and Information Systems (CIS) capability, able to support all nations' defence requirements and achieved in an affordable and cost-effective way.

103. PURPOSE OF THIS PUBLICATION

The purpose of the ACP 140 is to provide the technical interoperability standards for achieving the CCEB vision. The primary aim is to facilitate interoperability among CCEB Nations so that their defence CIS (supporting different elements within the CCEB business) can exchange information and other services in a timely and secure manner, as determined by business and operational imperatives.

In meeting these objectives it is vital that all systems adhere to a common security framework so that each affords appropriate protection to information held within the CCEB CIS federation. Such a federation will be composed of diverse CIS, including fixed and deployed Intranets belonging to the national systems. For joint operations these networks have to be linked together to provide the technical means for interworking.

This publication also seeks to expose some of the rationale supporting the selection of services and standards. The complete rationale is given in the 'CITA Rationale and Development Framework' document, ref. CCEB Publication 1007.

104. NATIONAL COMPLIANCE WITH ACP 140

ACP 140 is intended to guide the planning of acquisition and development of specific service functions within new or upgraded national CIS, where there is a need to interoperate with the systems of other CCEB nations. It should be consulted by project managers and systems designers to ensure compliance with essential aspects of the CITA, and by operational staff seeking to exploit the interoperability provided by the CITA.

ACP 140 is a "forward-looking" document listing the standards agreed for relevant services and interfaces to be used now and in the future. It also serves as a baseline for the migration of existing systems towards CITA compliance. The document provides a CCEB agreed coherent set of services and standards that can be used to support interoperability between CCEB nations. It does not seek to constrain the designer to this set of services and standards when meeting system requirements; the designer is free to use whatever is appropriate within the system. However it does identify the services and standards that must be present at the system boundary in order for interoperability to be realised.

The selected standards do not cover all aspects of CIS, nor do they include all information technology standards used currently within national systems. The CITA is concerned only with services essential for interworking between nations. However, any other standards specified outside the scope of ACP 140 must be additive, complementary, and non-conflictive with ACP 140 and its applicable Annexes and Supplements.

Legacy Systems

If legacy standards are needed to interface with existing systems, they can be implemented on a case-by-case basis in addition to the mandated standards. New systems should aim to be backwards compatible wherever possible. Legacy systems should aim to migrate towards CITA standards when upgrades are due.

105. DOCUMENT ORGANISATION

Allied Communications Publications (ACPs) provide the specific instructions and procedures essential to the conduct of common military operations. They are prepared in accordance with the format contained in the ACP 198 series.

Sections I - IV of the present document explain the context for ACP 140 and the processes by which CIS standards have been selected to meet CCEB requirements for interoperability. Implementation and Compliance are covered in Section V. Individual CIS service areas are discussed in separate chapters within Section V and detailed technical specifications given for each service area within CITA scope.

106. NATIONAL POINTS OF CONTACT

Each nation has a lead in the development and maintenance of the CITA as follows:

Australia:
Mr. Jed Bartlett
Technical Architect,
Information Policy and Plans Branch,
Defense Information Systems Group
Department of Defence
NCC-B12-3, Canberra, ACT 2600.
Tel. +61 2 6266 3671
Fax +61 2 6266 4574
Email: jed.bartlett@defence.gov.au

Canada:
Capt. Grant L. Griswold
Directorate Information Management and Strategic Division, DIMSD 5-3-2,
National Defence Headquarters,
Ottawa, Ontario, K1A 0K2.
Tel. +1 613 945 0952
Email: Capt.G.Griswold@debbs.ndhq.dnd.ca

New Zealand:
Mr. Mark Baddeley
JCIS,
HQNZDF,
Private Bag,

Wellington.
Tel. +64 4 496-0191
Email: markb@jcis.mil.nz

United Kingdom:
Mr. John Keefe
EC(CCII) RSG
Northumberland House
Northumberland Avenue
London, WC2N 5BP.
Tel. +44 171 21 87458
Email: dcisseg4@dgics.mod.uk

United States:
Mr. Charles Schaffer
JS/J6I, C4 Systems Directorate Technology and Architecture Division,
Room 1E833, The Pentagon,
Washington DC, 20340-0001.
Tel. +1 703 614 7005
Email: cschaffer@acm.org

SECTION II - CITA OVERVIEW

107. ARCHITECTURES

An architecture is defined by the Institute for Electrical and Electronic Engineers (IEEE) in IEEE 610.12 as the organisational structure of a system or component, their relationships, and the principles and guidelines governing their design and evolution over time. The CITA has defined an interrelated set of architectures: Operational, Systems, and Technical. Figure 1-2 shows the relationship among the three architectures. The definitions are provided here to ensure a common understanding of the three architectures[1].

[1] These definitions are based on the US definition. In the UK the Operational Architecture is further broken down into the Business Architecture and Information Architecture

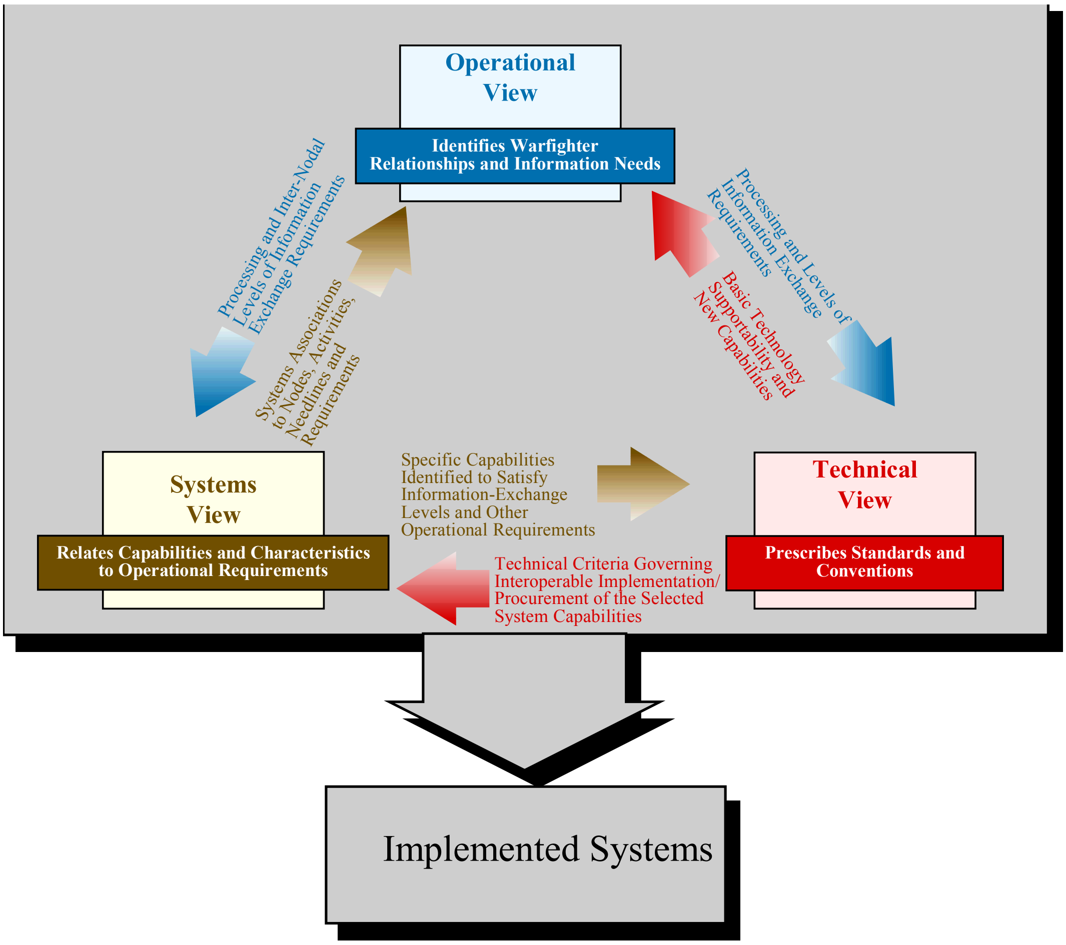
Operational View
Identifies Warfighter Relationships and Information Needs
Processing and Inter-Nodal Levels of Information Exchange Requirements
Systems Associations to Nodes, Activities, Needlines and Requirements
Processing and Levels of Information Exchange Requirements
Basic Technology Supportability and New Capabilities
Systems View
Relates Capabilities and Characteristics to Operational Requirements
Specific Capabilities Identified to Satisfy Information-Exchange Levels and Other Operational Requirements
Technical View
Prescribes Standards and Conventions
Technical Criteria Governing Interoperable Implementation/ Procurement of the Selected System Capabilities
Implemented Systems

Figure 1-1. Architecture Relationships

a. Operational Architecture View (OA)

A description (often graphical) of the operational elements, assigned tasks, and information flows required accomplishing or supporting the warfighting function. It defines the type of information, the frequency of exchange, and what tasks are supported by these information exchanges.

b. Systems Architecture View (SA)

A description, including graphics, of systems[2] and interconnections[3] providing for or supporting warfighting functions. The SA defines the physical connection, location, and identification of the key nodes, circuits, networks, warfighting platforms, etc., and specifies system and component performance parameters. It is constructed to satisfy Operational Architecture requirements per standards defined in the Technical Architecture. The SA shows how multiple systems within a subject area link and interoperate, and may describe the internal construction or operations of particular systems within the architecture. (C4 Chiefs Consensus SA Definition, 12 January 1996, as modified at the suggestion of the USD(A&T) community).

c. Technical Architecture View (TA)

A minimal set of rules governing the arrangement, interaction, and interdependence of the parts or elements whose purpose is to ensure that a conformant system satisfies a specified set of requirements. The technical architecture identifies the services, interfaces, standards, and their relationships. It provides the technical guidelines for implementation of systems upon which engineering specifications are based, common building blocks are built, and product lines are developed.

The CITA corresponds to the technical architecture of this model.

108. CITA OVERVIEW

a. Definition

The CITA is the Technical Architecture that contains the technical recommendations for a profile of standards and guidelines for support of essential requirements for interoperability among CCEB nations.

As noted above, a technical architecture is simply a list of information services and their corresponding standards. The intent of standardising on services is to promote interoperability across any systems designed using this architecture. The CITA is the technical architecture endorsed by CCEB nations.

[2] Systems: People, machines, and facilities organized to accomplish a set of specific functions, which cannot be further subdivided while still performing required functions. Includes the radios, terminals, command, control, and support facilities, sensors and sensor platforms, automated information systems, etc., necessary for effective operations.

[3] Interconnections: The manual, electrical, or electronic communications paths/linkages between the systems. Includes the circuits, networks, relay platforms, switches, etc., necessary for effective communications.

Although there are many information services that could contribute to interoperability, an attempt has been made to limit recommendations to those services for which an operational requirement currently exists and for which suitably open standards are available. For newer technology services which are not yet part of an operational concept or for which standards are still emerging, some discussion is provided, but no recommendation.

CCEB Publication 1007, *CITA Rationale and Development Framework*, describes the process by which candidate information services were identified and evaluated. In determining the necessity of each service, the following are considered: relevance to interoperability, existence of an inter-nation requirement, and scale of the inter-nation requirement. The feasibility of each service is determined by considering whether there exists an acceptably open standard, the interconnection security policy, legacy issues, cost, risk, and system evolution issues. It is recognised that it is not always advantageous to standardise a particular service.

The standards selection process has sought to adopt wherever possible those services and standards that are dominant in the commercial world and which benefit from wide market support.

The results of the process are summarised in Table 2-2 "CITA Specification (Version 2.0)".

b. CITA Concept of Operations

The CITA is relevant when the need arises to transfer information or share services between a system belonging to one CCEB nation and a system belonging to another CCEB nation. The standards defined in the CITA are required at one of the following:

1. the boundary of the national system (typically a gateway);

2. the interface between a deployed system and the target CCEB system; or

3. within a CCEB coalition system (the national system becomes part of the coalition system).

c. Benefits

The benefits of adopting the CITA result from the advantages of a technical architecture and the use of mainstream commercial products. In summary they are as follows:

- interoperability is promoted when common standards are adopted;
- there is increased scope for the use of commercial, off-the-shelf (COTS) products, hence reduced cost and risk;

- there is a reduced risk of lock-in to a single system provider;
- system evolution is made easier by following commercial developments.

d. Relationship to National Technical Architectures

Clearly, the Nation Specific Interoperability Technical Architectures (NSITAs), and any alternative forms of local agreement relevant to other nations, must embrace the CITA: This concept is depicted in Figure 1-2 below.

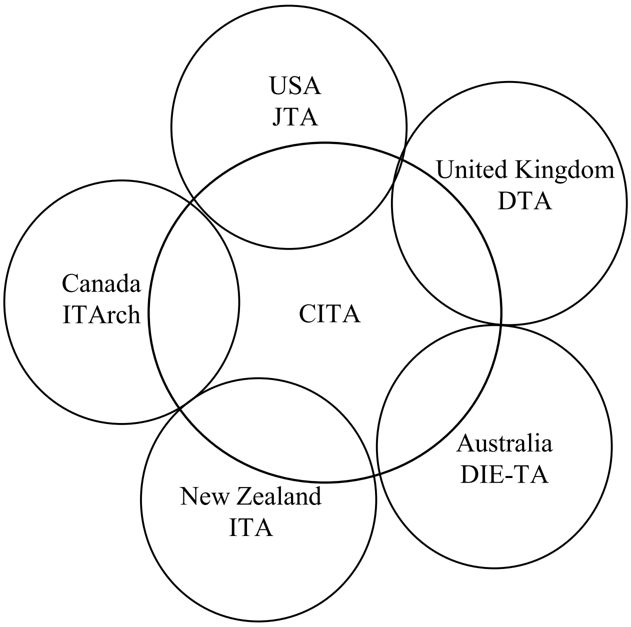

Figure 1-2. Scope of the CITA in relation to other NSITAs

e. Security

The CITA makes no statements about the security architecture or policy to be adopted for end-systems. However, the widespread interconnection of systems envisaged means that secure messaging alone cannot provide adequate protection. Depending upon the protective marking of the data and/or system and the geographical location and nature of the communications bearers, messaging interconnections between systems will continue to require COMSEC protection through the use of (an appropriate grade of) encryption at the network/link level or at the application layer level. Even where the data exchanged has a low or even no security classification, COMPUSEC concerns, possibly derived from distant systems in the federation, will often lead to a supplementary requirement for network-level encryption.

f. Technical Scope of the CITA

The technical scope of the CITA will establish where the boundary between it and nation-specific ITAs lies. This will depend largely on the interoperability mechanisms CITA aims to employ. A service will be deemed *outside* the CITA if the need to use it (and hence standardise it) arises solely from requirements within individual nation boundaries. Conversely, a service is a *candidate* for standardisation within the CITA whenever there is a significant requirement for exchange of that service between CIS from different CCEB nations.

A balance must be established between the benefits and restrictions of standardisation. Where a limited number of CIS are involved, an ad hoc bilateral, or multilateral, agreement may be preferable. The *principles* by which it is proposed that issues such as these should be decided are discussed in Paragraph 111.

The technical architecture does not constitute a complete specification of the system. The CITA addresses only those elements of CIS that are relevant to interoperability between CCEB nations and these may be a relatively small part of the full system functionality. National ITAs probably go beyond the scope of CITA but they are still limited to interoperability issues.

At the very least, each system will offer applications specific to the needs of its local users. Furthermore, there will be locally required infrastructure services for which standardisation (either within the CITA or a nation-specific ITA) would serve no useful purpose. In these cases, local service agreements will be negotiated between the parties involved and standards chosen according to purely local requirements, taking note of sector level preferences (Land Sea or Air) or, for example ABCA agreements[4].

[4] Of course, what may start out as local agreements may find wider utility. In this case, these local agreements may be adopted and subsumed by the CITA depending on the scale and scope of their applicability. The overall objective is to move towards commonality.

SECTION III - STANDARDS SELECTION PROCESS

109. SELECTION PROCESS OVERVIEW

The CITA standards selection process consisted of the following four stages:

a. CITA Candidate IT Services are identified

b. CITA Scoping Principles are applied

c. CITA Scope is assessed

d. CITA Standards are recommended.

This process is depicted diagramatically below in Figure 1-3.

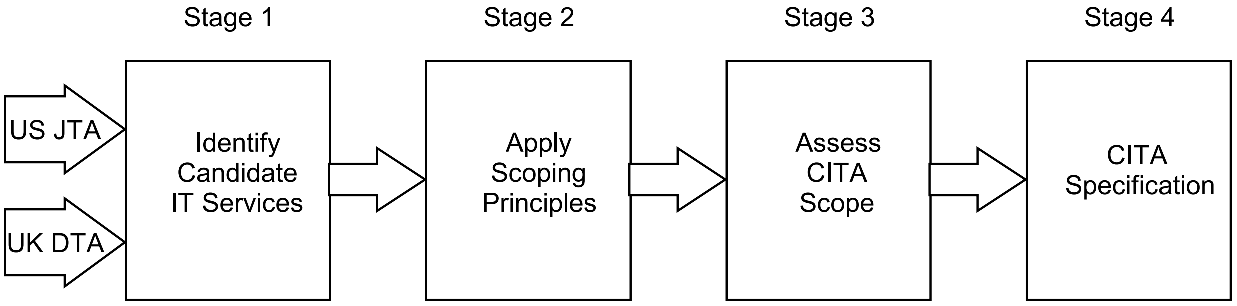

Figure 1-3: Overview of CITA Standards Process

110. CANDIDATE IT SERVICES

The initial set of candidate IT services were selected from nation-specific technical architectures defined by the US and the UK, namely the DoD JTA and the MOD DTA respectively.

The candidate IT services were categorised as follows:

a. Operating Systems Services

This category covers standards for the services provided by computer operating systems and the means of accessing them by user applications.

b. User Interface Services

This category covers a miscellany of standards relevant to the Human-Computer Interface, including look and feel standards/conventions, APIs for windowing systems, desktop managers plus desktop hardware and operating system environments. It includes remote presentation protocols (e.g. X11) and inter-process communication protocols (e.g. DDE) which are also listed under Distributed Computing.

c. Network Services[5]

This category covers the standards for communications-related applications operating at layer 7 of the ISO OSI reference model. It also includes some of the services and protocols required by these applications.

d. Communications

This category covers the standards for transporting data between end systems. It includes the bearers of data, both physical (e.g. fibre-optic) and non-physical (e.g. RF).

e. Distributed Computing

This category covers the services required to access and distribute information, resources and processing across a federation of systems.

f. Data Management Services

This category covers the services required to manage shared data, data dictionaries and databases. It includes the services required for database replication and remote data access.

g. Data Interchange

This category covers the standards for the interchange of information between systems and applications. It can include standards that are supported natively by several applications as well as intermediate standards that applications can convert both to and from

h. System and Network Management

This category covers the services required to effectively manage the configuration, security and faults of end systems and their interconnecting networks.

[5] Network services do not equate to the 'Network Layer' in the OSI model.

i. Software Engineering

This category mainly covers standards for the system/software lifecycle processes and associated tools but also includes standards for programming languages and their bindings.

j. Graphics

This category provides standards for graphics services providing users and user applications with the means to create, store, access, manipulate, display and print graphic images.

k. Internationalisation

This category covers standards and conventions that facilitate the use or re-use of systems or software within different National or cultural contexts.

l. Security Services

This category covers the services required to provide secure communications between CIS. They also provide services for detecting and preventing hostile manipulation and attack of CIS.

m. Support Application Software

This category covers general-purpose or utility applications software. A variety of application types are included under this heading. Those covered explicitly under this heading are OA applications and those categorised as transaction processing applications.

n. Collaborative computing

This category covers services and applications that support group-working by spatially separated individuals. They promote the ability of coalition forces to collaborate using their respective CIS.

o. Special Application Software

This category covers system or mission-specific applications software which would only be expected to be found on systems performing a similar role.

111. SCOPING PRINCIPLES

The resultant set of IT services that passed through the first filter were then scrutinised against a set of scoping principles. These principles were designed to evaluate whether an IT service should be considered by the CITA for possible standardisation. The scoping principles used were as follows

a. **Inter-Nation requirement**: is there genuine evidence of an existing or emerging requirement to exchange this service across systems from different nations?

b. **Openness**: is there an open solution available to provide this service or are there overriding business or operational reasons for adopting a non-open solution?

c. **System boundary issues**: which parts of a standard, or what types of standard, are applicable to the specification of external system interfaces?

d. **Legacy issues**: are there practical concerns related to legacy systems that would limit standardisation or suggest a preferred standard?

e. **Cost/risk**: are there significant cost and risk implications of standardisation in this area?

f. **Interconnection security policy**: are there likely to be interconnection security policy constraints that would prevent systems exchanging these services, or the adoption of particular standards?

g. **System evolution**: do system evolution imperatives dictate that standardisation is not feasible, or that multiple versions of any given standard needs to be supported concurrently?

112. ASSESSMENT OF SCOPE

Having applied the second filter, the resultant IT services were analysed and a potential set of standards identified. From the potential standards, well defined, well supported and reasonably stable standards were allocated to the CITA IT services. Also identified were emerging CITA IT standards that were considered too immature at present for inclusion now, but were expected to become dominant in the near term. In a number of cases there are a number of competing, emerging standards. Further market analysis is required before a decision can be made for their inclusion into the CITA.

SECTION IV - IMPLEMENTATION

113. APPLICABILITY AND COMPLIANCE

The CITA is applicable to national CIS that are required to participate in a CCEB-wide CIS federation, exchanging information across national boundaries and possibly between CCEB nation forces during combined operations. However, not every participating CIS will necessarily implement the whole of the CITA because national operational requirements for that CIS may not require all the CITA services or its services are supported with other products.

The extent to which a particular system implements the CITA services determines its scope for interoperability with other CITA-compliant systems. A fundamental principle of CITA compliance is that where a CIS offers a service for interworking across CCEB nations, that service will be implemented according to the CITA specification. However, there will be different levels of CITA compliance according to the actual services involved.

a. Acquisition

CCEB nations must include checks within their CIS procurement procedures to ensure that when participating systems are developed or modified, they are compliant with the CITA according to the claimed interoperability level. Typically this will involve four stages:

1. Before a system is developed or modified, the project manager will create a CITA-compliant standards profile for the system which will be continually updated as the project proceeds;

2. The system developer will select specific options within the CITA standards used by the system in order to provide the necessary functionality and interoperability level;

3. The standards profile will be submitted for internal approval. If any waivers are granted on CITA-specified standards for whatever reason, the CITA WG should be informed so that the impact of non-compliance on CCEB federation interoperability can be assessed;

4. After approval, the standards profile should form an integral part of the procurement specification and confirmation should be sought, by inspection and testing, that the standards are implemented correctly in the delivered system. Periodic monitoring of the system during its service life should be undertaken to see that CITA compliance to a given interoperability level is maintained.

b. Interoperability levels

Interoperability levels have been agreed by the CITA group. A progressive scale of CIS functionality has been defined with identified points on the scale corresponding to common system capabilities. The lowest levels of the scale will apply to systems offering basic interconnection and simple data exchange, whilst the upper end of the scale will be used to describe sophisticated systems with full network interconnection, able to work with complex data objects across the CIS federation[6].

The interoperability levels are shown in Table 1-1.

Table 1-1

Interoperability Level	Name	Description
1a	Basic document exchange	OA document interchange, hypertext, character sets/alphabets, graphics/still and moving images, file compression, page description, security labelling, accounting and audit.
1b	Full document exchange	As for 1a plus military transfer formats, military symbols (codes only) and standard data products.
2a	Network connection	Inter-networking, transport and domain name services.
2b	Basic Intranet connection	File transfer and interpersonal email with attachments[7].
2c	Web connection	Hypertext transfer, on-line publishing and news group services. Security labelling syntax, semantics and positioning within published documents. Also web authentication and access control mechanisms.
2d	Organisational messaging	Organisational messaging based on X.400 as defined in ACP 123. Also messaging security services.
2e	Directory services	Directory services based on X.500 as defined in ACP 133.

[6] It is possible that hardware compliance will have to be addressed separately from service compliance; these matters are still under discussion.

[7] The CCEB requirement for interpersonal email has recently been agreed.

Interoperability Level	Name	Description
3a	Secure database access/exchange	Database management, remote database access, data dictionary, CCEB data model and associated security services.
3b	Distributed applications	Distributed computing, object interfaces and object middleware if relevant. Also database replication, information sharing, collaborative computing and special applications.

Level 1 compliant systems can read and write files in the formats cited; transfer is either manual or through dedicated links.

Level 2 compliant systems should be able to connect to a CCEB Intranet and perform web access, email, and formal messaging. Level 1 and 2 together broadly equate to NATO level 4 interconnection.

Level 3 compliance is outside the current CITA scope but should fall within the emerging CITA.

A statement showing the level of compliance with CITA will be required for every participating national CIS, so that its scope for interoperability within the CCEB federation becomes apparent. Nations will assume responsibility for carrying out compliance checks on their own systems and issuing compliance statements to the CITA WG. Ideally, compliance with at least one of the defined CITA levels should be mandatory but allowance will have to be made for possible exceptional factors until experience with CITA systems has been gained.

114. CITA EVOLUTION

The CITA will be kept under review and changes introduced to the specification in response to new CCEB requirements and technology developments. Service areas presently outside the scope of CITA should be monitored for possible inclusion, while the standards for existing services must reflect changes in the market. Market movements will affect the feasibility of implementing services in accordance with open standards and this factor must be taken into account in revising the CITA specification. The need to retain backwards compatibility is recognised; market forces and the need to retain a customer base will frequently ensure that commercial products are compatible with earlier versions as well as competing products.

A major change driver will be feedback obtained from projects compliant with the CITA. Nations must establish mechanisms, if not already in place, for eliciting feedback and passing relevant information to the CITA WG to assist CITA management. In any event, evolution of the CITA specification will have to take into account changes to national technical architectures where they relate to CITA functionality.

The CITA WG will monitor these change drivers and update the CITA as appropriate.

Proposed changes and comments are to be put to national contacts. These will be considered on a regular basis by the CITA Working Group and appropriate action taken.

This page intentionally blank

CHAPTER 2

CITA SPECIFICATION SUMMARY

201. CITA SPECIFICATION

Table 2-2 summarises the recommended standards profiles for the CITA. The services have been grouped into 15 broad categories. For each service, there is a recommendation for a standard. A more detailed rationale for selecting that standard is included in CCEB Publication 1007.

202. KEY DRIVERS

A key driver in the process of selecting the CITA services has been the existence (or likely existence) of user requirements and whether or not the technology exists to provide those services. The selection of standards for the CITA specification has been driven by the following:

a. **adoption of Internet and web technologies.** The CITA cites the popular internetworking standards TCP, IP and UDP; the data exchange protocols in widespread use on the Internet and in commercial networks (HTTP, NNTP, FTP etc.); and common data interchange formats (HTML, JPEG, zip, etc.);

b. **need for security.** The most significant departure from commercial standards is in the adoption of a common security protocol (ACP 120) particularly in support of messaging. A common approach to secure messaging is fundamental to the existence of an effective CITA;

c. **adoption of essential requirements to meet military needs.** Common elements of CCEB standards for organisational messaging (ACP123) and directory (ACP133) are adopted.

203. CITA SERVICES OUT OF SCOPE

A number of CITA services are currently ruled out of scope; they are not shown in the specification summary but are listed below. Services are ruled out of scope if there is no inter-nation requirement or there are no acceptable standards. The scope of CITA services will be kept under review by the Working Group.

Table 2-1

No.	Service Area	Service	Ref Para	Page
1.	Operating System Services		301.	3-1
2.	User Interface Services		401.	4-1

No.	Service Area	Service	Ref Para	Page
3.	Distributed Computing	Distributed process	703.	7-2
4.		Remote presentation	704.	7-3
5.		Distributed file services	705.	7-4
6.		Distributed time services	706.	7-4
7.		Distributed print services	707.	7-5
8.		Distributed transaction processing	708.	7-6
9.		Distributed object services (object middleware)	710.	7-8
10.		Distributed system management	711.	7-9
11.	Data Management Services	Data dictionary services	804.1	8-4
12.		Database management services	804.2	8-4
13.	System and Network Management	System management	1002.	10-1
14.		LAN management	1003.	10-1
15.		National WAN management	1004.	10-2
16.		Communications bearer system management	1006.	10-4
17.	Software Engineering Services		1101.	11-1
18.	Graphics	Graphics programming languages and APIs	1202.	12-1
19.		Application software having a drawing capability	1203.	12-2
20.	Internationalisation		1301.	13-1
21.	General Security	Security domian mediation	1509.	15-9
22.	Support Applications Software		1601.	16-1
23.	Collaborative Computing	Workflow services	1702.	17-1
24.		Whiteboarding	1705.	17-4
25.	Special Applications Software	Geographical Information Systems	1802.	18-1
26.		Track management	1803.	18-2
27.		Alert services	1804.	18-3
28.		Data fusion	1805.	18-4

204. MULTIPLE STANDARDS

The CITA specification generally identifies a single standard or group of interdependent standards for each service. In some cases, however, the Working Group agreed that it would be appropriate to specify multiple standards which progressively add functionality (e.g. HTML, XML & SGML). In